

U.S. Department of Justice

United States Attorney
Southern District of New York

MEMO ENDORSED

United States Courthouse
300 Quarropas Street
White Plains, New York 10601

October 28, 2020

BY EMAIL and ECF

Honorable Kenneth M. Karas
United States Courthouse
Southern District of New York
300 Quarropas Street
White Plains, NY 10601

Re: *United States v. Spyros Panos*, 18 Cr. 581 (KMK)

Dear Judge Karas:

The Government respectfully writes to raise issues it would like to address at the October 29, 2020, final pretrial conference in the above-captioned case. First, to simplify the trial and limit the number of witnesses appearing in the Courthouse, the Government would like to pre-authenticate certain Government Exhibits, which are comprised of records provided by Google LLC ("Google"). Second, the Government objects to the admission of proposed defense exhibits.

A. Government Exhibits Consisting of Records Provided by Google are Authentic and Admissible under FRE 902(11)

Government Exhibits 110 and 400 through 589 are subscriber records and all emails in the relevant time period from the Gmail account with the user name ydo.excelorthopedics (the "Gmail Account"). These records are returns from Google in response to a search warrant and a 2703(d) Order, and were accompanied by the certificates of authenticity attached hereto as Exhibit A.

Federal Rule of Evidence ("FRE") 902 addresses "evidence that is self-authenticating." FRE 902. "No extrinsic evidence of authenticity" is required for this evidence "to be admitted." *Id.* Courts in the Second Circuit regularly admit self-authenticating evidence pursuant to Rule 902 without witness testimony. *See, e.g., United States v. Komasa*, 767 F.3d 151, 156–57 (2d Cir. 2014) ("we conclude that the district court properly admitted the mortgage loan files as self-authenticating documents" pursuant to Rule 902(11)). Certified domestic records of a regularly conducted activity may be self-authenticated pursuant to Rule 902(11) provided the records satisfy the business records requirements of 803(6)(A)-(C), as shown "by a certification of the custodian or another qualified person that complies with a federal statute or a rule prescribed by the Supreme Court." *United States v. Rom*, 528 F. App'x 24, 27 (2d Cir. 2013).

Rule 803(6), in turn, provides that business records are admissible if they are accompanied by a certification of their custodian or other qualified person that satisfies three requirements: (A) that the records were “made at or near the time by—or from information transmitted by—someone with knowledge”; (B) that they were “kept in the course of a regularly conducted activity of a business”; and (C) that “making the record was a regular practice of that activity.” *Id.*

Here, Google has certified both that the records in Government Exhibits 110, and 400 through 589 are true and correct copies of records maintained by Google, and that Google’s servers record the data contained in the records “automatically at the time, or reasonably soon after, it is entered or transmitted by the user, and this data is kept in the regular course of this regularly conducted activity and was made by regularly conducted activity as a regular practice of Google.” *See* Exhibit A: Feb. 6, 2018, Certification ¶ 4, Apr. 30, 2018, Certification ¶ 5. These certifications comply with Rule 803(6).

Numerous court have granted motions *in limine* finding similar electronic service provider records authentic pursuant to Rule 902(11). *See, e.g., United States v. Denton*, 944 F.3d 170, 183 (4th Cir. 2019) (“we are unpersuaded that Denton’s Sixth Amendment right to confront witnesses includes ‘the right to confront a records custodian who submits a Rule 902(11) certification’ of a business record”), *cert. denied*, 140 S. Ct. 2585 (2020); *United States v. Gal*, 606 F. App’x 868, 875 (9th Cir. 2015) (affirming the admission of “emails based on Yahoo’s affidavit” pursuant to FRE 902(11)); *United States v. Hassan*, 742 F.3d 104, 133 n.25 (4th Cir. 2014) (rejecting “appellants’ contention that the Facebook and Google certifications are insufficient because they were made for litigation purposes several years after the postings occurred” as “entirely unpersuasive.”); *United States v. Hitt*, No. 2:15-CR-117-GEB, 2018 WL 288013, at *2 (E.D. Cal. Jan. 4, 2018) (granting the government’s motion *in limine* pursuant to Rule 902(11) with respect to “subscriber and login information from Yahoo!” and “IP records from AT&T”); *United States v. Jones*, No. CR 15-174, 2016 WL 10704381, at *3 (E.D. La. Feb. 17, 2016) (“the records provided by Netspend; Facebook; Google; Marriott Residence Inn—New Orleans, Louisiana; and Samsung, as described more fully by the government in its papers, are admissible business records under the Federal Rules of Evidence.”)

Although these records are Google’s business records because they were (a) “made at or near the time by—or from information transmitted by—someone with knowledge;” (B) “kept in the course of a regularly conducted activity of a business”; and because (C) “making the record was a regular practice of that activity,” the government is *not* arguing that the *content* of the communications in the Gmail Account fits into the *hearsay exception* for business records. This is because Google’s employees generally do not have any information about the substance of the communications in the Gmail Account, only the reliable method by which the records (including to/from data, email content, and other user generated content) were created, transmitted, and maintained as an essential part of Google’s businesses. Thus, the government intends to argue at trial that the substance of these communications is admissible as non-hearsay, or as hearsay fitting into a different hearsay exception, such as the admission of a party opponent (FRE 801(d)(2)(A)).

B. The Defendant's Proposed Exhibits Must be Authenticated

On Thursday, October 22, 2020, defense counsel delivered to the Government a flash drive containing approximately 1,000 proposed Defense Exhibits – some of which contain documents of 2000 pages. As described below, many of the proposed exhibits are irrelevant. Others were provided to the Government without any documentation from record custodians to establish authenticity. They do not appear to be documents obtained by the Government in connection with its investigation. Tellingly, although the Government made several requests for authentication information, the defendant has failed to provide any certifications or other indicia of authenticity. Further, the defense has refused to disclose how the records were obtained at all. As described below, we have conducted a limited investigation and have preliminarily concluded that at least some of the proposed Defense Exhibits appear to be fraudulent documents. The following are just examples of some of the proposed Defense Exhibits and reasons for our objections. We have not addressed every exhibit submitted to us by the defense.

First, proposed Defense Exhibits A1 through A223, B1, B6 through B80, C1 through C15, C35, C36, C41, and C51 through C54, appear to be peer review reports regarding the medical treatment of individual claimants, copies of peer review checks to Excel O LLC that are not authenticated, and medical summaries. These records are not relevant to the charges, *i.e.*, whether the defendant stole the identity of a practicing doctor and defrauded medical peer review companies, and therefore should not be admitted into evidence.

Second, proposed Defense Exhibits E1, E3, E5, E8, E18, E22, E24, E27, E28, E29, E30, E144, and E593, purportedly are emails to/from an AOL account with the user name “panosmdl@aol.com,” used by the defendant. Despite the Government’s repeated requests, the defendant has not provided information establishing the authenticity of these emails. The Government did not obtain records regarding this email account during its investigation and cannot independently establish the authenticity of the exhibits. In an attempt to determine whether these emails are authentic, the Government asked the purported senders of two of the emails, proposed Defense Exhibits E30 and E144,¹ to review their email servers and confirm the existence of the emails. Because the emails purportedly are from several years ago, neither purported sender was able to locate the emails in accessible records. However, the purported sender of proposed Defense Exhibit 30 indicated the email was forged.

Consequently, the Government served a 2703(d) Order on Oath Inc., AOL’s parent company. Yesterday, the Government obtained records from Oath that show that Oath does not have “to/from” information related to either email although their records do reflect that other emails were sent and received in the same time period. Because we believe these email records are fraudulent, the Court should require the defense to provide evidence establishing the authenticity of these records including by providing the Government with the emails in native format. When the Government asked defense counsel where these emails came from he replied that he could not answer that question. Should the defense fail to provide evidence of

¹ Proposed Defense Exhibits E30 and E144 are attached hereto as Exhibit B.

The Honorable Kenneth M. Karas

October 28, 2020

authenticity, the Court should preclude the defense from offering Defense Exhibits E1, E3, E5, E8, E18, E22, E24, E27, E28, E29, E30, E144, and E593 into evidence at trial.

Third, proposed Defense Exhibits E2, E4, E6, E7, E9-E17, E19-E21, E23, E25, E26, E31-143, E144-E592 and E594-E618 consist of emails that purportedly are to/from the Gmail Account. Many of them are not individual emails but instead are threads of multiple emails. The Government cannot individually authenticate the hundreds of Gmail emails that the defendant has proposed by comparing them against the Gmail records obtained from Google. Thus, we cannot agree to stipulate to the authenticity and admissibility of these proposed exhibits. However, the Government intends to offer all the emails contained in the Gmail Account, during the relevant time period, as Government Exhibit 400, so all the emails should be in evidence in any event. As described above, the contents of Government Exhibit 400 were obtained from Google and have been authenticated by Google. In addition, the Government has indicated that it will assist the defense in accessing particular emails within Government Exhibit 400 during trial. Thus, the Court should preclude the defense from offering proposed Defense Exhibits E2, E4, E6, E7, E9-E17, E19-E21, E23, E25, E26, E31-143, E144-E592 and E594-E618, which are unauthenticated records.

Fourth, proposed Defense Exhibit G12 is a form entitled Request to Staff Form purportedly submitted by the defendant to his unit counselor on June 16, 2014 (the "Request to Staff Form"), while the defendant was incarcerated at USP Canaan.² The purported Request to Staff Form seeks credit for time supposedly served between April 2, 2014, and April 7, 2014, and contains a notation that the request was granted. The Government anticipates offering records and witness testimony at trial to establish the defendant surrendered to serve his sentence for his first conviction on April 7, 2014, and questioned the provenance of proposed Defense Exhibit G12. The Government conferred with the Bureau of Prisons and learned that such forms ordinarily are maintained in an inmate's "correspondence" file. The Government requested a copy of the defendant's correspondence file and learned that the Request to Staff Form is not in the defendant's correspondence file. In addition, the Government conferred with the case manager and unit manager assigned to the defendant at USP Canaan. Each stated that the signature on the form is not his signature, and could not identify the signature as belonging to another staff member. Finally, we have learned that there is no indication in Bureau of Prisons records that the Request to Staff Form was ever acted upon; the defendant's sentence does not appear to have been recomputed to provide credit for the days noted in the Request to Staff Form. Thus, the Government is unable to verify the authenticity of proposed Defense Exhibit G12 and believes it is also a fraudulent document. The Court should require the defense to provide the Court with evidence establishing the authenticity of these records and, should the defendant fail to provide such evidence, preclude the defense from offering proposed Defense Exhibit G12.

² Proposed Defense Exhibit G12 is attached hereto as Exhibit C.

The Honorable Kenneth M. Karas


October 28, 2020

Fifth, proposed Defense Exhibits H1 and H2 appear to be screen shots of file folders from unknown digital files, which are unauthenticated and appear irrelevant. Defense Exhibits H3-H150 appear to contain PDF files of proposed Government exhibits, each of which has an open properties window misleadingly obscuring the Government exhibit, but not the Government Exhibit sticker. The authenticity of these files has not been established. The properties depicted in the proposed Defense Exhibits are untethered from the properties of the Government's actual exhibits as they exist in the Government's files, and the Government has no mechanism for establishing what the properties are related to or where they came from.

As to the remaining proposed Defense Exhibits, at a minimum, we request that the Court order the defense to provide authentication information and its arguments as to relevance for all exhibits the defense proposes to seek to offer into evidence at trial prior to trial. We also request that the Court order the defense to provide any proposed exhibits containing electronic evidence in native format.

The Court will address these and other evidentiary issues at the final pre-trial conference on 10/29/20. Defendant should be prepared to provide the basis to authenticate the exhibits discussed herein.

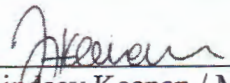
So Ordered.


10/28/20

Respectfully submitted,

AUDREY STRAUSS
Acting United States Attorney

by:


Lindsey Keenan / Margery Feinzig
Assistant United States Attorneys
(914) 993-1907 / 1903

cc: Lawrence Fisher, Esq. (by email and ECF)